

REMARKS

Applicants cancel claims 6 and 9. Claims 1-5, 7-8, and 10-12 remain pending in the application. Applicants amend claims 1-2 to incorporate features that correspond to those of claims 6 and 9. No new matter has been added.

Claims 1-12 were rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent Application Publication No. 2002/0188720 to Terrell et al. in view of U.S. Patent No. 5,941,947 to Brown et al. Applicants amend claims 1-2 to incorporate features that correspond to those of claims 6 and 9, and respectfully traverse the rejection.

The Examiner cited paragraph [0046] of Terrell et al. as allegedly disclosing the features recited in claim 9. Page 6, paragraph 9 of the Office Action. Such portion of Terrell et al. only includes, however, description of maintaining a profile and supporting a service level, or deleting the profile, according to the service level supported by the profile 222. Such portion of Terrell et al. is, therefore, silent on filter control duration time management. And, again, the Examiner only relied upon description in Brown et al. of a relational database having access rights and groupings for security purposes as alleged suggestion of the claimed “optimally deal with” features.

As such, even assuming, arguendo, that it would have been obvious to one skilled in the art at the time the claimed invention was made to combine Terrell et al. and Brown et al., such a combination would still have failed disclose or suggest,

“[a] network access control method for a network system comprising:
network apparatuses having packet filtering functions;
a service server connected with an IP network via the network apparatus, providing contents on the service server to a user;
a user terminal connected with the IP network via the network apparatus, for the user to utilize the contents on the service server;
a reception server connected with the IP network via the network apparatus, receiving an access request to the

contents on the service server from the user on behalf of the service server; and

an access control server controlling the network apparatus for a limitation of the access request to the contents on the service server,

said method comprising the steps of:

a) said access control server first denying all the access requests directed to the contents on the service server via the network apparatus;

b) said reception server receiving access request information to the contents on the service server from said user terminals, and registering the received access request information in an access list; and

c) said access control server extracting such an amount of the received access request information from said access list, based on a processing capability of the service server and a traffic amount for the service server, as that said service server can optimally deal with, and performing traffic control to the network apparatus connected with the user terminals so as to allow the user terminals to directly access the contents on the service server in the other of access requests, wherein

said access control server comprises:

an access information database holding information concerning the processing capability of the service server and a maximum permissible access number calculated based on the processing capability of the service server;

a traffic control part controlling the network apparatus;

a static permissible access number calculating part calculating the maximum permissible access number based on the information concerning the processing capability of the service server;

a filtering optimizing part reading such an amount of the access request information from the access list holding the access request information from the user terminals in the reception server, from the top, as that for the maximum permissible access number, producing packet filtering setting information for the users making access requests to be able to access to the service server, and setting the produced information in the network apparatus via said traffic control part;

an effective timer setting part setting an effective timer for the access request information when the packet filtering setting information is produced; and

a filtering canceling part canceling the packet filtering control set in the network apparatus, when the

effective timer has expired,” as recited in claim 1.
(Emphasis added)

Accordingly, Applicants respectfully submit that claim 1 is patentable over Terrell et al. and Brown et al., separately and in combination, for at least the foregoing reasons. Claim 2 incorporates features that correspond to those of claim 1 cited above, and is, therefore, together with claims 3-5, 7-8, and 10-12 dependent therefrom, patentable over the cited references for at least the same reasons.

In view of the remarks set forth above, this application is in condition for allowance which action is respectfully requested. However, if for any reason the Examiner should consider this application not to be in condition for allowance, the Examiner is respectfully requested to telephone the undersigned attorney at the number listed below prior to issuing a further Action.

Any fee due with this paper may be charged to Deposit Account No. 50-1290.

Respectfully submitted,

/Dexter T. Chang/
Dexter T. Chang
Reg. No. 44,071

CUSTOMER NUMBER 026304
Telephone: (212) 940-6384
Fax: (212) 940-8986 or 8987
Docket No.: 100794-11710 (FUJI 18.503)
DTC:tb